Japan Patent Office,
Unexamined Patent Application Publication No. H7-200756

PUBLICATION DATE: August 4, 1995

[TITLE OF THE INVENTION]

PORTABLE TYPE DATA CARRIER PROCESSING SYSTEM

[Object] To prevent the illegal use of a security card extracted during a session.

[Constitution] Write completion information indicating the successful completion of a session to security card 30 for authenticating user card 20. In a case that security card 30 is extracted illegally during the session, completion information remains in "incompletion". A host terminal prevents access to data even if security card 30 is inserted in the host terminal; as a result, the illegal use of the card is prevented beforehand.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平7－200756

(43)公開日　平成７年(1995)８月４日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｋ　17/00		S		

審査請求　未請求　請求項の数１　ＦＤ　（全　５　頁）

(21)出願番号　特願平5－349861

(22)出願日　平成５年(1993)12月28日

(71)出願人　000003193
凸版印刷株式会社
東京都台東区台東１丁目５番１号

(72)発明者　由良　彰之
東京都台東区台東一丁目５番１号　凸版印刷株式会社内

(72)発明者　高橋　正志
東京都台東区台東一丁目５番１号　凸版印刷株式会社内

(72)発明者　松村　秀一
東京都台東区台東一丁目５番１号　凸版印刷株式会社内

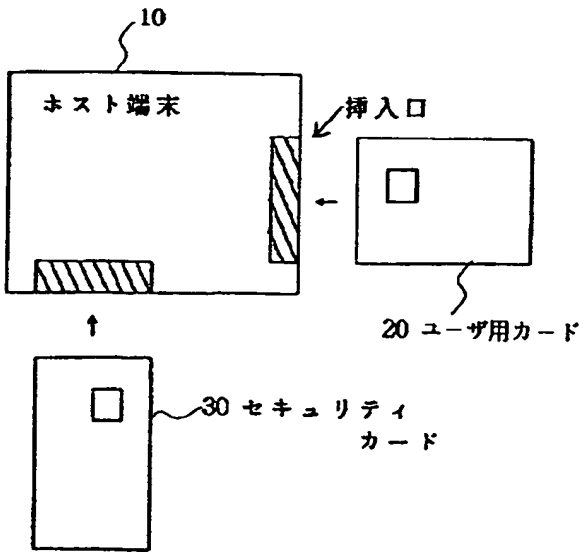
(74)代理人　弁理士　安倍　逸郎

(54)【発明の名称】　可搬型データ担体処理システム

(57)【要約】

【目的】　セッション途中で抜き取られたセキュリティカードの不正使用を防止する。

【構成】　ユーザ用カード２０の認証等を行うセキュリティカード３０に、セッションの正常終了を表す終了情報を書き込む。セッションの途中でセキュリティカード３０が不正に抜き取られた場合には、終了情報は「未終了」のままとなる。このセキュリティカード３０をホスト端末に挿入したとしても、ホスト端末はデータのアクセスを禁止するため、不正使用を未然に防止することができる。



1

【特許請求の範囲】

【請求項１】　可搬型データ担体と、

可搬型データ担体の認証を行った後に可搬型データ担体に対してデータのアクセスを行うホスト端末とを備えた可搬型データ担体処理システムにおいて、

上記可搬型データ担体は終了情報記憶手段を備え、ホスト端末は以下の(1)～(4)の処理を実行することを特徴とする可搬型データ担体処理システム。

(1)ホスト端末が可搬型データ担体を認証した場合には、ホスト端末は終了情報記憶手段に「未終了」のデータを書き込む。

(2)可搬型データ担体に対するデータのアクセスが正常に終了した場合には、ホスト端末は終了情報記憶手段に「終了」のデータを書き込む。

(3)ホスト端末が可搬型データ担体を認証する際に終了情報記憶手段に「終了」のデータが書き込まれていた場合には、ホスト端末は可搬型データ担体に対するデータのアクセスを許容する。

(4)ホスト端末が可搬型データ担体を認証する際に終了情報記憶手段に「未終了」のデータが書き込まれていた場合には、ホスト端末は可搬型データ担体に対するデータのアクセスを禁止する。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、可搬型のデータ担体処理システム、詳しくは移動通信等において使用されるＳＩＭ（Ｓｕｂｓｃｒｉｂｅｒ　Ｉｄｅｎｔｉｔｙ　Ｍｏｄｕｌｅ）、金融アプリケーションにおけるＳＡＭ（Ｓｅｃｕｒｅ　ＡｐｐｌｉｃａｔｉｏｎＭｏｄｕｌｅ）、もしくはＩＣカード等の可搬型データ担体処理システムに関する。

【０００２】

【従来の技術】近年、移動通信、金融アプリケーション等の分野においては、持ち運び容易なＳＩＭ、ＳＡＭ、ＩＣカード等の可搬型データ担体が使用されている。例えば、金融アプリケーション等の分野において使用が検討されているＳＡＭは、セキュリティを必要とするアプリケーションプログラムの一部、例えば暗号・復号プログラムが書き込まれたＩＣカード等の可搬型データ担体であって、一般ユーザ使用のカードとは別のものである。

【０００３】このような可搬型データ担体は、ホスト端末の挿入口に差し込まれ、両者の鍵が一致するか否かを判断することにより可搬型データ担体の正当性が確認される。そして、可搬型データ担体が正当であると認証された場合には、ホスト端末においてセッション等のデータのアクセスが行われる。このとき、可搬型データ担体には、正当な認証が行われたことを表すデータ、認証用のＫｅｙデータ、乱数のデータ等が書き込まれる。

【０００４】しかしながら、セッションが終了する前

2

に、可搬型データ担体をホスト端末から抜き取った場合には、可搬型データ担体は正当であると認証された状態のままである。したがって、抜き取られた可搬型データ担体を他のホスト端末等に挿入した場合、このホスト端末においてデータのアクセスが許可されてしまう。すなわち、可搬型データ担体等のセキュリティ機能の部分のみを不正に抜き取られた場合、他のホスト端末において不正使用されるおそれが生じる。すなわち、この可搬型データ担体をホスト端末に挿入した際に、認証用のＫｅｙデータ、乱数のデータの交換等がされることなく、セッションが行われてしまう。金融アプリケーション等においては、このような問題は特に重大である。

【０００５】

【発明の目的】そこで、本発明は、可搬型データ担体処理システムにおいて、セッションの途中において抜き取られた可搬型データ担体の不正使用を禁止することを目的としている。

【０００６】

【課題を解決するための手段】請求項１に記載の発明は、図１に示されるように、可搬型データ担体１と、可搬型データ担体の認証を行った後に可搬型データ担体に対してデータのアクセスを行うホスト端末２とを備えた可搬型データ担体処理システムにおいて、上記可搬型データ担体は終了情報記憶手段３を備え、ホスト端末２は以下の(1)～(4)の処理を実行することを特徴とする可搬型データ担体処理システムである。

【０００７】(1)ホスト端末２が可搬型データ担体１を認証した場合には、ホスト端末２は終了情報記憶手段３に「未終了」のデータを書き込む。(2)可搬型データ担体１に対するデータのアクセスが正常に終了した場合には、ホスト端末２は終了情報記憶手段３に「終了」のデータを書き込む。(3)ホスト端末２が可搬型データ担体１を認証する際に終了情報記憶手段３に「終了」のデータが書き込まれていた場合には、ホスト端末２は可搬型データ担体１に対するデータのアクセスを許容する。(4)ホスト端末２が可搬型データ担体１を認証する際に終了情報記憶手段３に「未終了」のデータが書き込まれていた場合には、ホスト端末２は可搬型データ担体１に対するデータのアクセスを禁止する。

【０００８】

【作用】請求項１に記載の発明において、ホスト端末が可搬型データ担体を認証した場合には、ホスト端末は終了情報記憶手段に「未終了」のデータを書き込む。そして、正当権限者による非活性化命令によって可搬型データ担体に対するデータのアクセスが正常に終了した場合には、ホスト端末は終了情報記憶手段に「終了」のデータを書き込む。このようにして正当な権限者により正常終了した可搬型データ担体を、再度ホスト端末に挿入したとする。この場合には、終了情報記憶手段に「終了」のデータが書き込まれているため、ホスト端末は可搬型

データ担体に対するデータのアクセスを許容する。一方、データのアクセスが正常に終了する前に可搬型データ担体を不正に抜き取った場合には、終了情報は「未終了」の状態のままである。したがって、この可搬型データ担体を再度ホスト端末に挿入した場合、ホスト端末は可搬型データ担体に対するデータのアクセスを一切禁止し、可搬型データ担体の使用は不可能になる。これにより不正に抜き取られた可搬型データ担体を利用した不正行為を未然に防止することができる。

【０００９】

【実施例】以下に、本発明の一実施例を図面を参照しながら説明する。

【００１０】図２は本実施例に係る可搬型データ担体処理システムの外観構成図である。この可搬型データ担体処理システムは、ホスト端末１０、ユーザ用カード２０、セキュリティカード３０を備えて構成されている。ホスト端末１０は、ユーザ用カード２０に対してデータの読み書きを行うものであって、暗号化・復号化および認証処理等を実行するＣＰＵ、アプリケーションプログラム等が書き込まれたメモリ等により構成されている。また、ホスト端末１０には、ユーザ用カード２０、セキュリティカード３０が挿入される挿入口を備えている。

【００１１】ユーザ用カード２０は、金融情報等のデータを保持するものであって、データの暗号化・復号化等を行うマイクロコンピュータおよびトランザクションファイル等を記憶する不揮発性メモリ等を内蔵している。このユーザ用カード２０は各ユーザが所持するものである。

【００１２】セキュリティカード３０もまた、マイクロコンピュータおよび不揮発性メモリを備えて構成されている。このセキュリティカード３０は、主としてサービスを提供する者が所持するもので、ホスト端末１０に挿入されたユーザ用カード２０が正当なものであるか否か、また、ホスト端末１０が受信したデータが正当であるか否かを確認する機能を備えている。不揮発性メモリは、電気的消去可能なＥＥＰＲＯＭ、あるいは、バッテリバックアップされたスタティックＲＡＭ等により構成されている。また、セキュリティカード３０には、外部からアクセス不可能な不揮発性メモリを備え、この不揮発性メモリには後述する終了情報が書き込まれている。終了情報は、前回のセッション中においてセキュリティカード３０が不正に抜き取られた場合には「未終了」の状態となるものである。よって、この終了情報を確認することによりセキュリティカード３０の不正使用を防止することが可能となる。

【００１３】なお、セキュリティカード３０と同等の機能を、図３のセキュリティ処理装置４０として実現することも可能である。セキュリティ処理装置４０はホスト端末１０にインタフェース等を介して接続されており、ホスト端末１０から切り離すことが可能なものである。

【００１４】図４は、本実施例に係る可搬型データ担体処理システムにおける処理の概要を表す図である。相互認証は、ユーザ用カード２０が正当なものであるか否かを確認する処理であり、この相互認証は、端末ホスト１０がユーザ用カード２０およびセキュリティカード３０のそれぞれの暗号化したデータ（鍵）等が一致するか否かにより行われる。また、ユーザ用カード２０は、取引に伴い電子署名を生成し、この電子署名はセキュリティカード３０により確認される構成となっている。

【００１５】以上のように構成された可搬型データ担体処理システムの作用を図５に示されるフローチャートを参照しながら説明する。

【００１６】サービス提供者がセキュリティカード３０をホスト端末１０の挿入口に挿入すると、ホスト端末１０からセキュリティカード３０に電源が供給され、セキュリティカード３０が活性化する（Ｓ１）。次に、ホスト端末１０は、セキュリティカード１０に記録された終了情報が「終了」を表しているか否かを確認する（Ｓ２）。

【００１７】この終了情報は、前回のセッションが正常に終了したか否かを表すフラグであって、セッションが正常に終了しないうちにセキュリティカード３０をホスト端末１０から引き抜いた場合には終了情報は「未終了」の状態のままとなる。ホスト端末１０は、読み取った終了情報が「未終了」であった場合（Ｓ２でＮＯ）には、一切応答することなく以後のアクセスを禁止する（Ｓ３）。これにより、セッション途中で抜き取られ、認証された状態のままのセキュリティカード３０を利用した不正使用を防止することができる。なお、無応答の処理は、無限ループ等を利用することにより実現可能である。一方、終了情報が「終了」であった場合（Ｓ２でＹＥＳ）には、ホスト端末１０は、セキュリティカード３０内の終了情報を「未終了」に書き換え（Ｓ４）、ステップＳ５以後の処理を実行する。

【００１８】ステップＳ５において、ホスト端末１０はコマンドの送信をセキュリティカード３０に許可し、コマンドが送信されてくるのを待機する。ホスト端末１０が、コマンドを受信すると（Ｓ６でＮＯ）、受信したコマンドが非活性化命令のコマンドであるか否かを判断する（Ｓ７）。非活性化コマンドでない場合（Ｓ７でＮＯ）には、セッションコマンド等の処理を実行し（Ｓ１３）、レスポンスを送信する（Ｓ１４）。そして、再び、ホスト端末１０は新たなコマンドが送信されてくるのを待機する（Ｓ５）。一方、ステップＳ７において、ホスト端末１０が非活性化コマンドを受信した場合（Ｓ７でＹＥＳ）には、このコマンドとともに受信した鍵とセキュリティカード３０内の参照鍵とを照合する（Ｓ８）。

【００１９】両者が一致しなかった場合（Ｓ９でＮＯ）には、ホスト端末１０は、一致しなかった旨のレスポン

5

スを送信し（Ｓ１４）、新たなコマンドを待機する（Ｓ５）。両者が一致した場合（Ｓ９でＹＥＳ）には、上述した終了情報を「終了」に書き換える（Ｓ１０）。そして、ホスト端末１０は、レスポンスを送信した後（Ｓ１１）、セキュリティカード３０を非活性化し（Ｓ１２）、全ての処理を終了する。

【００２０】したがって、本実施例によれば、終了情報を参照することにより、セキュリティカード３０がセッション途中で抜き取られたものか否かを判断でき、このセキュリティカード３０を利用した不正使用を未然に防止することが可能となる。なお、図３に示すように、セキュリティカード３０と同等の機能を有するセキュリティ処理装置４０について本発明を適用することも可能である。また、ホスト端末１０の内部にセキュリティ処理装置４０が配設されている場合においても、セキュリティ処理装置４０を切り離し、不正使用することも考えられることから、このような場合にも本発明を有効に適用することができる。

【００２１】

6

【発明の効果】以上説明してきたように、本発明によれば、可搬型データ担体処理システムにおいて、セッションが正常に終了したか否かを表す終了情報を確認することにより、セッション途中で抜き取られた可搬型データ担体の不正使用を未然に防止することが可能となる。

【図面の簡単な説明】

【図１】本発明に係る可搬型データ担体処理システムを表すブロック図である。

【図２】本発明の一実施例に係る可搬型データ担体処理システムのブロック図である。

【図３】本発明の一実施例に係る可搬型データ担体処理システムのブロック図である。

【図４】本発明の一実施例に係る可搬型データ担体処理システムのデータの流れを表す図である。

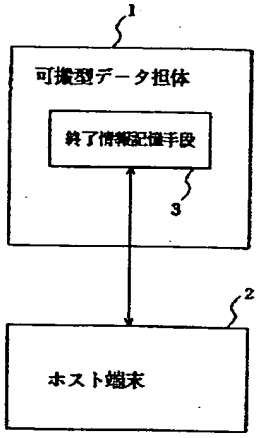
【図５】本発明の一実施例に係る可搬型データ担体処理システムの作用を表すフローチャートである。

【符号の説明】

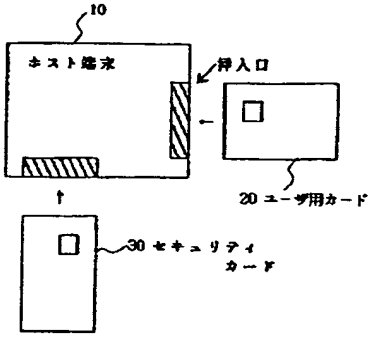
１０　ホスト端末

３０　セキュリティカード（可搬型データ担体）

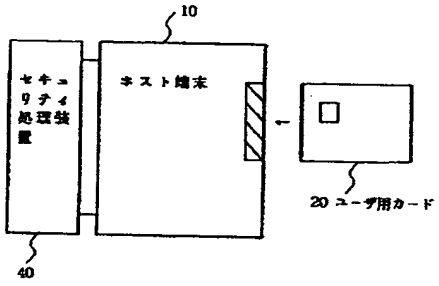
【図１】



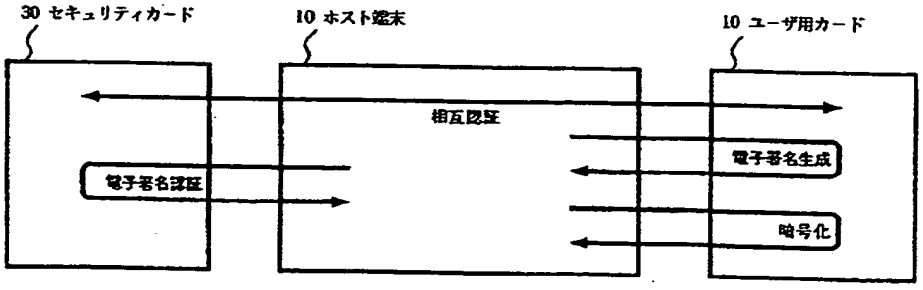
【図２】



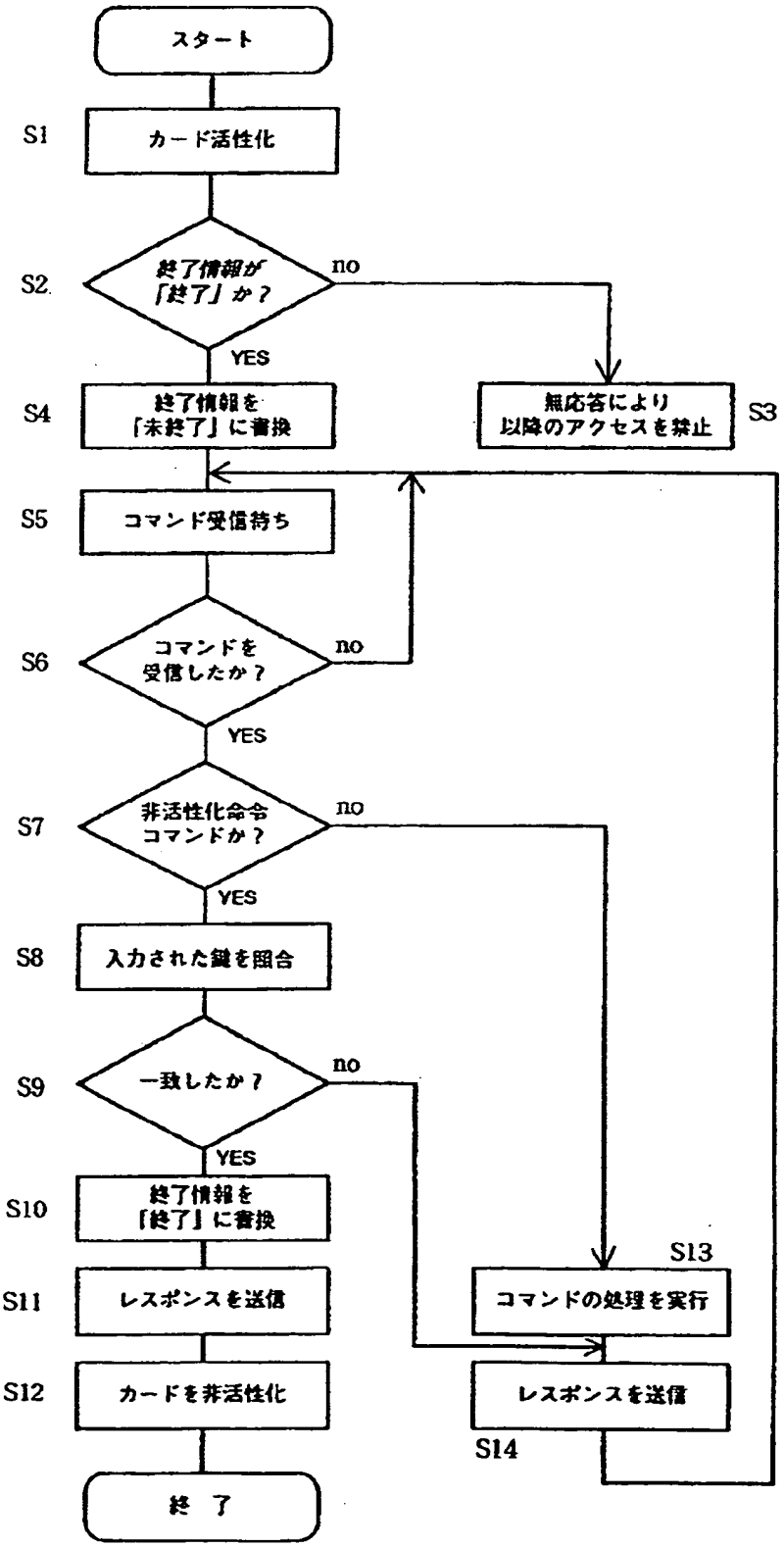
【図３】



【図４】



【図５】


スタート
S1
カード活性化
S2
終了情報が「終了」か？
no
YES
S4
終了情報を「未終了」に書換
S3
無応答により以降のアクセスを禁止
S5
コマンド受信待ち
S6
コマンドを受信したか？
no
YES
S7
非活性化命令コマンドか？
no
YES
S8
入力された鍵を照合
S9
一致したか？
no
YES
S10
終了情報を「終了」に書換
S11
レスポンスを送信
S12
カードを非活性化
終 了
S13
コマンドの処理を実行
レスポンスを送信
S14